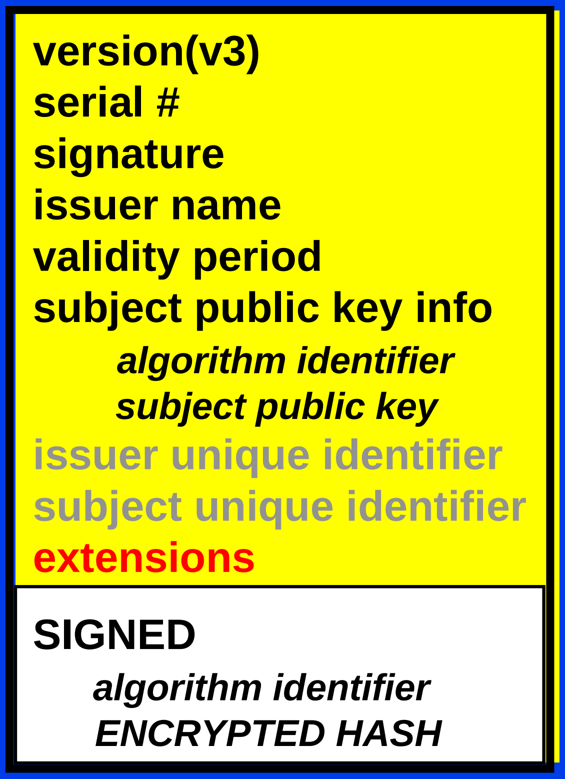
Federal Bridge CA Concept

Bill Burr
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
william.burr@nist.gov

EMA Challenge 2000 Demo

X.509 Certificate

- Version 3
  - extensions to help manage trust in complex PKI
- wide acceptance
  - many commercial products
  - basis for IETF PKIX RFC 2459

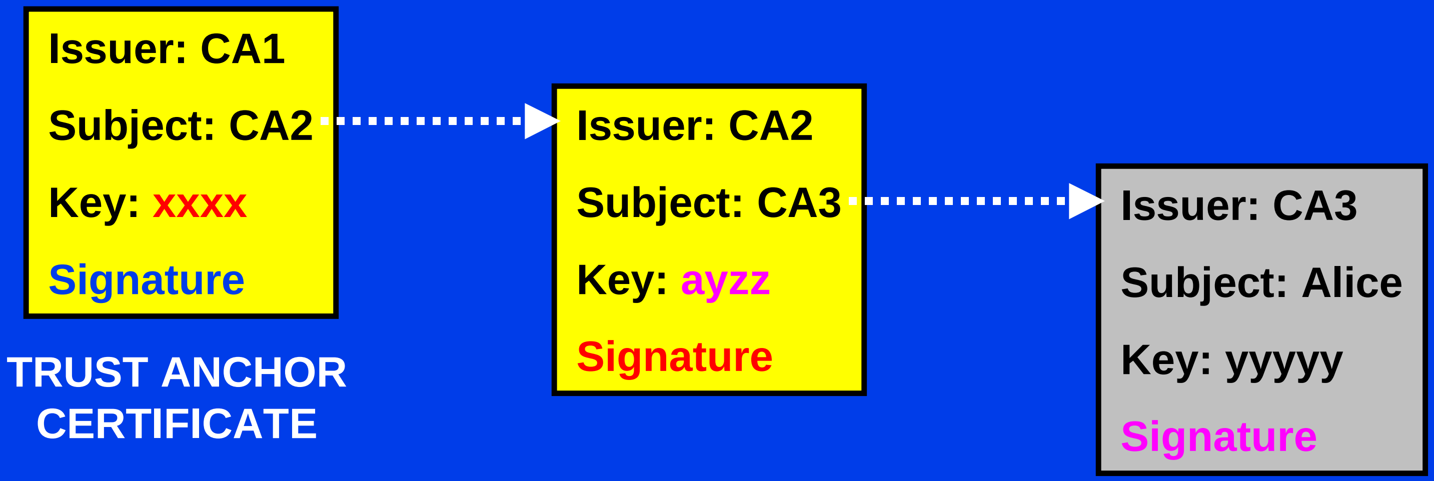


version(v3)
serial #
signature
issuer name
validity period
subject public key info
algorithm identifier
subject public key
issuer unique identifier
subject unique identifier
extensions

SIGNED
algorithm identifier
ENCRYPTED HASH

Certification Path

- Chain of certificates from trusted Certification Authority (CA) to end-entity



Issuer: CA1

Subject: CA2

Key: xxxx

Signature

TRUST ANCHOR
CERTIFICATE

Issuer: CA2

Subject: CA3

Key: ayzz

Signature

Issuer: CA3

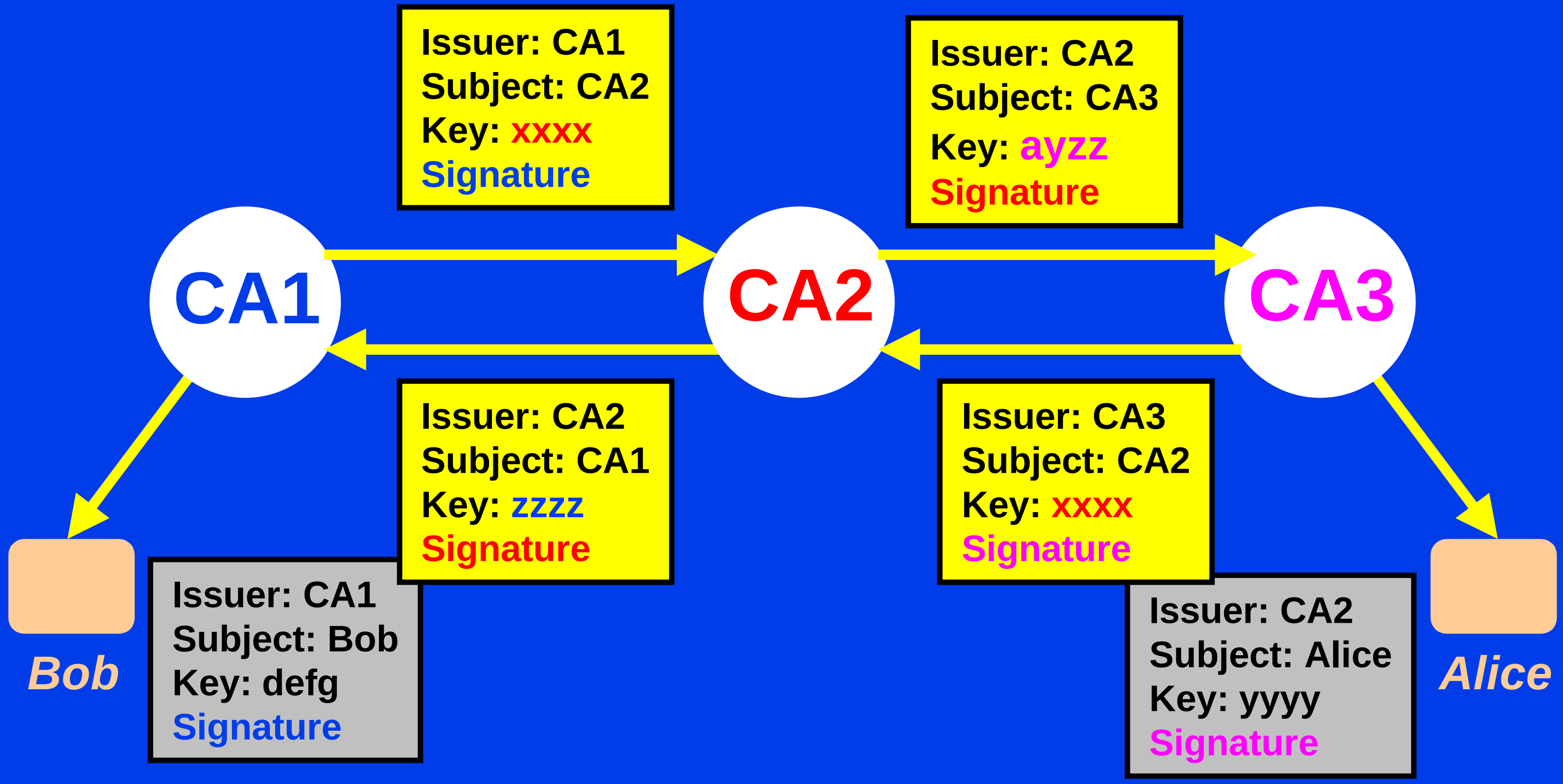
Subject: Alice

Key: yyyyy

Signature

Cross-certification

- CAs issue each other certificates



Issuer: CA1
Subject: CA2
Key: xxxx
Signature

Issuer: CA2
Subject: CA3
Key: ayzz
Signature

Issuer: CA2
Subject: CA1
Key: zzzz
Signature

Issuer: CA3
Subject: CA2
Key: xxxx
Signature

Issuer: CA1
Subject: Bob
Key: defg
Signature

Issuer: CA2
Subject: Alice
Key: yyyy
Signature

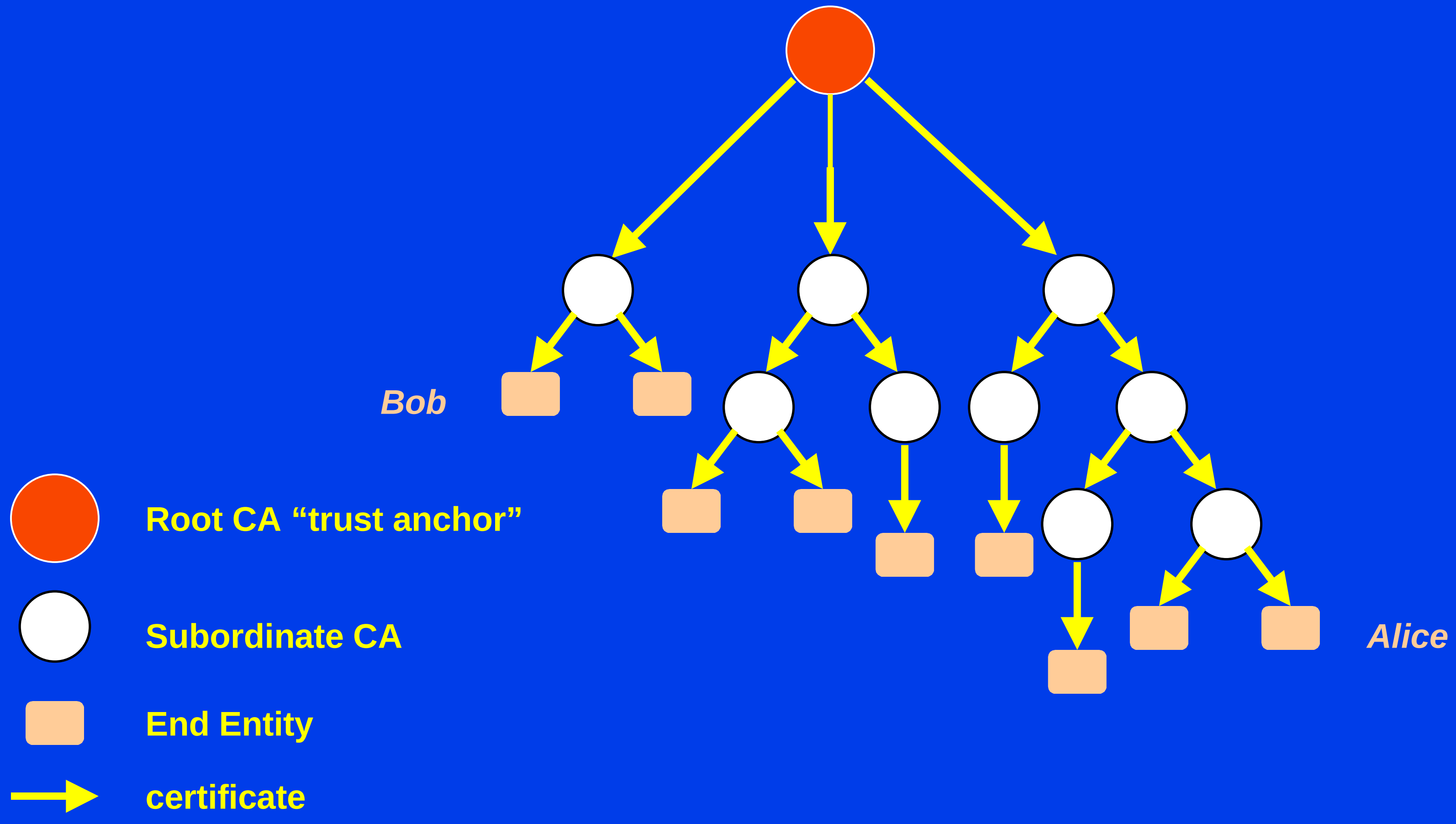
Certification Path Processing

- First find a path from “trust anchor” to signatory’s cert.
  - normally find certs. in directories
- Mechanical process:
  - a yes or no answer
    - additional info available to application
  - executed by relying party client
    - validate signatures and keys
      - key usage
    - cert. policies and name constraints
      - not implemented in most clients today

PKI "Topology"

- ◆ How can we arrange CA's and certificates to structure a PKI?
  - – At least 4 possibilities
    - » hierarchy
    - » mesh
    - » trust list
    - » Validation Authority (VA) based
  - – Aren't mutually exclusive

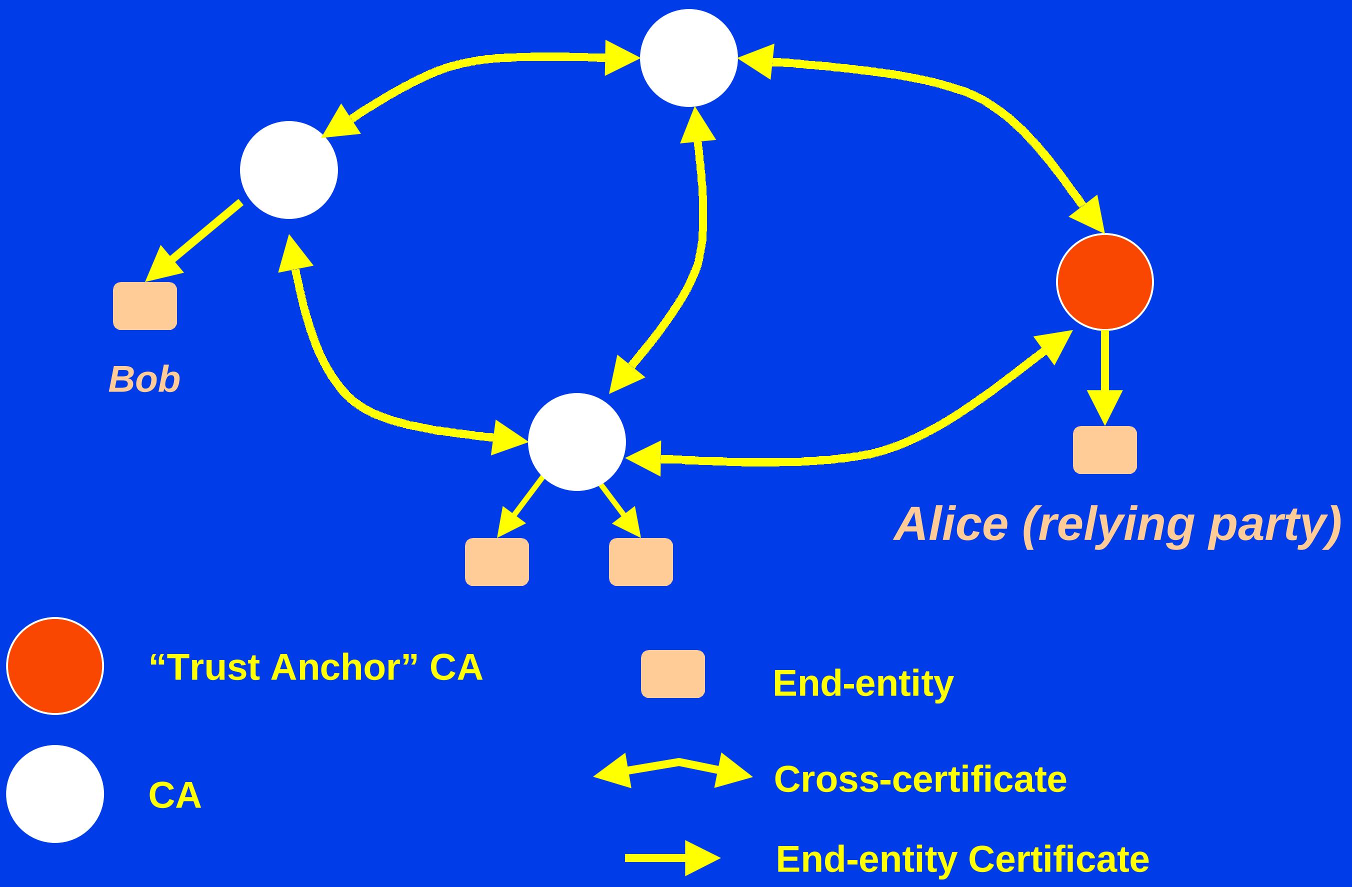
Hierarchical PKI



Hierarchical PKI

- All trust based on key of root CA
  - out of band root key distribution
  - root key compromise is disaster
- Relatively simple and efficient
- Mirrors many name & org structures
  - doesn’t mirror others
- Relatively good client support
- Who will be the root of roots?????

Mesh PKI (Alice’s view)



Bob

Alice (relying party)

● “Trust Anchor” CA

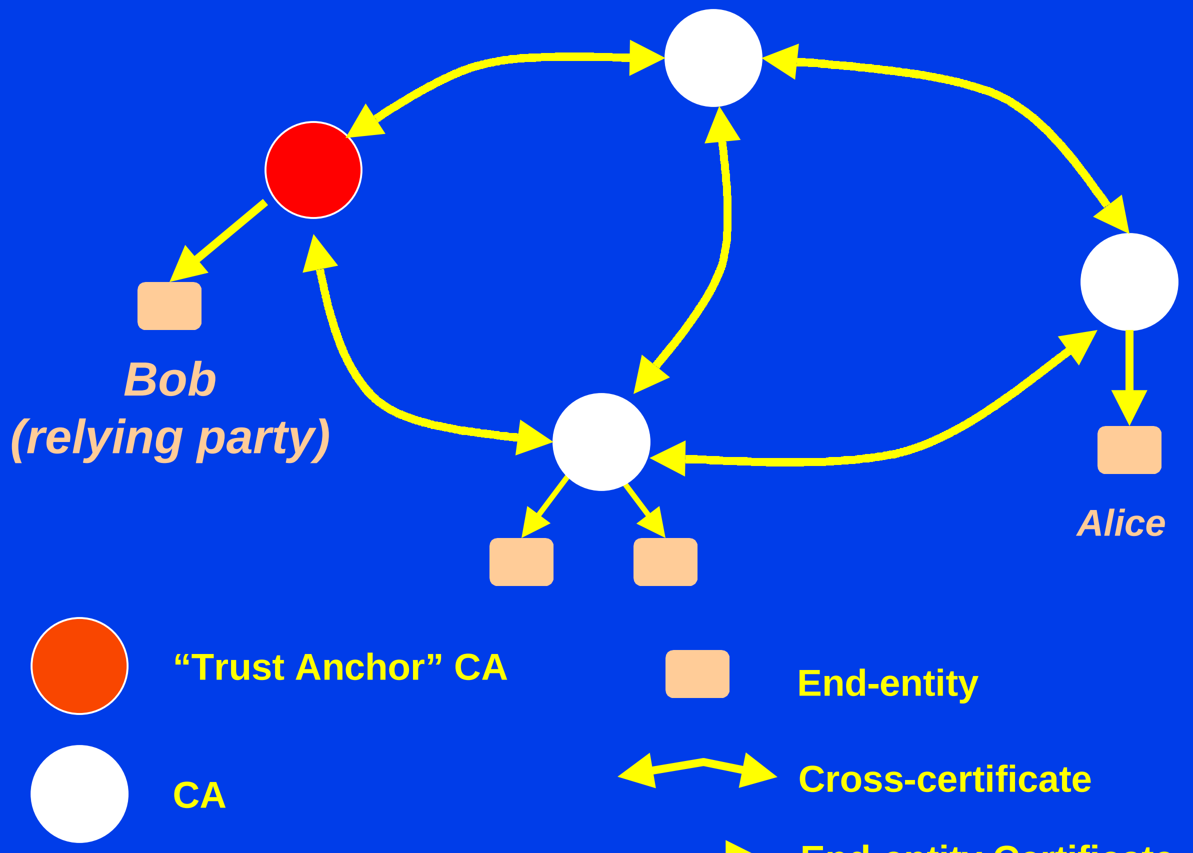
○ CA

▨ End-entity

↔ Cross-certificate

→ End-entity Certificate

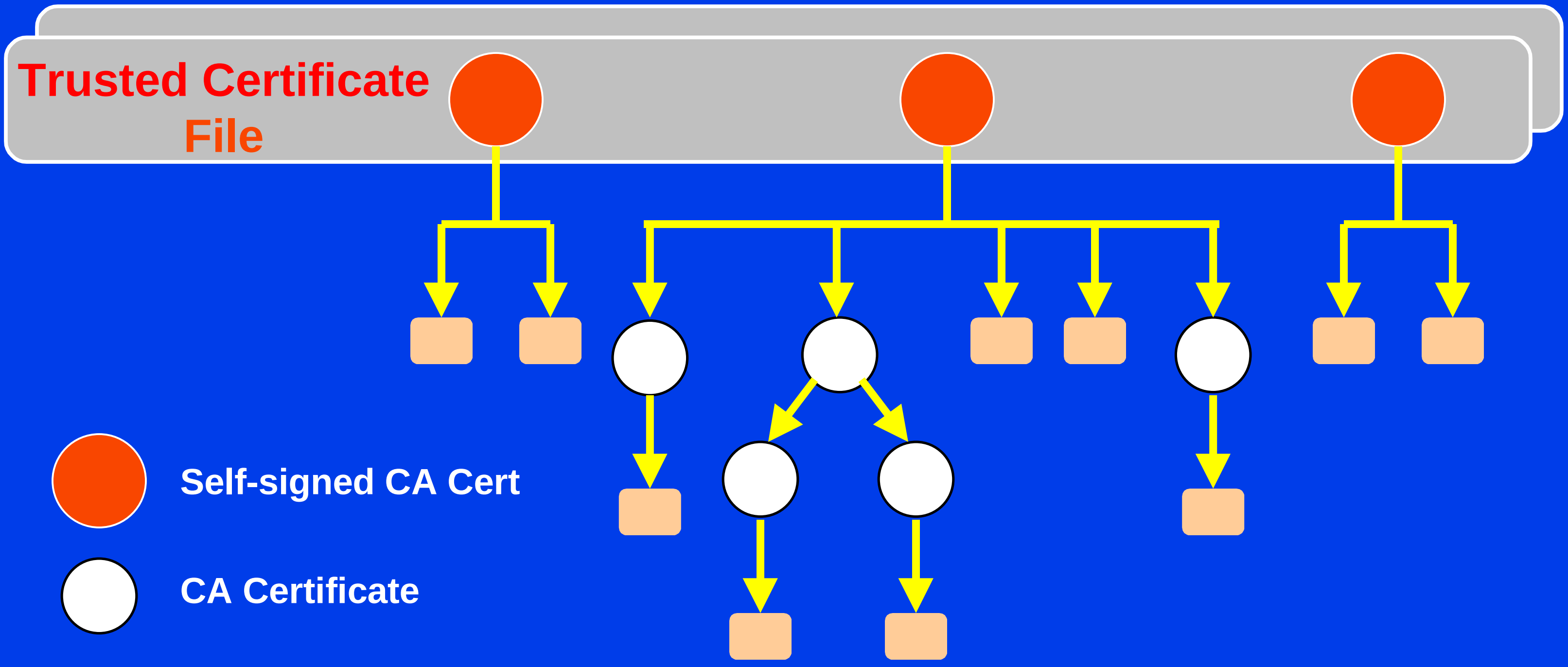
Mesh PKI (Bob’s View)



Mesh PKI

- CA’s cross-certify as peers
- Relying parties trust key of own CA
- Many organizations not hierarchical
  - Mirrors business arrangements between peers
- Finding certification paths a problem
  - need good directories
- Supported by some products

Trust List



Trusted Certificate File

🔴 Self-signed CA Cert

○ CA Certificate

🟧 End Entity Certificate

Trust List

- Predominates in WWW apps. today
  - major browsers
- Some clients can also use hierarchical certification paths
  - authority information access ??
- How do you manage the trust lists?
  - homogeneous environments maybe
  - heterogeneous environments a problem

NIST

Validation Authority Based

- Trust anchor is VA rather than CA
  - relying party trusts Cert if VA validates
    - » On-line Certificate Status Protocol (OCSP)
      - RFC 2560
      - how VA makes decision isn’t defined
- Trusted on-line server
  - performance & security implications
- Somewhat proprietary products
- Simplifies clients
- Facilitates other business models
  - relying party fee per transaction

Federal Government

- ◆ The world in microcosm
  - – many departments and agencies
    - » some large, some small
  - – different missions and structures
  - – largely independent of each other
- ◆ Different CAs going into agencies
  - – Agency PKI often application driven
    - » have to justify in terms of the specific app
  - – Some across agency for many apps

Bridge CA Approach

- Build the nexus to connect the pieces
- Three key elements:
  - Federal Policy Authority (FPA)
  - Federal “Bridge” CA (FBCA)
    - not a root!
    - cross certifies with CAs
    - may involve more than one CA product
  - Bridge CA Repository/Directory
    - for CA certificates and status

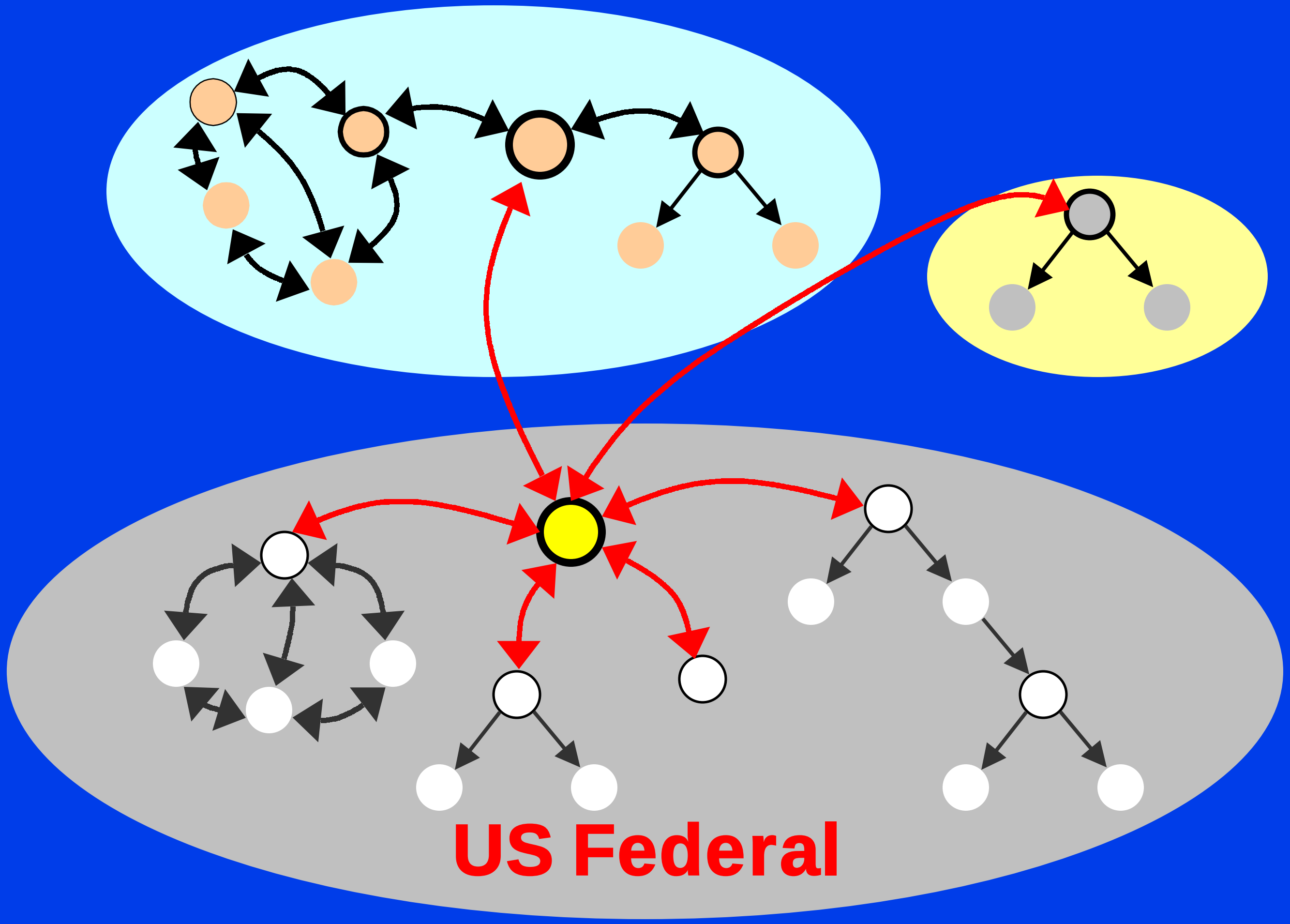
Federal Bridge CA (FBCA)

- Not a root CA!!!
  - not a trust anchor
- Will cross-certify with agency "principal CA's"
- Not necessarily a single CA product
- Managed by FPKI Policy Authority
- Operated by General Services Admin

FPKI Policy Authority

- Oversees BCA operation
- Voting members are agencies cross certified with BCA
- Evaluates agency certificate polices and makes cross-certification decisions and policy mappings

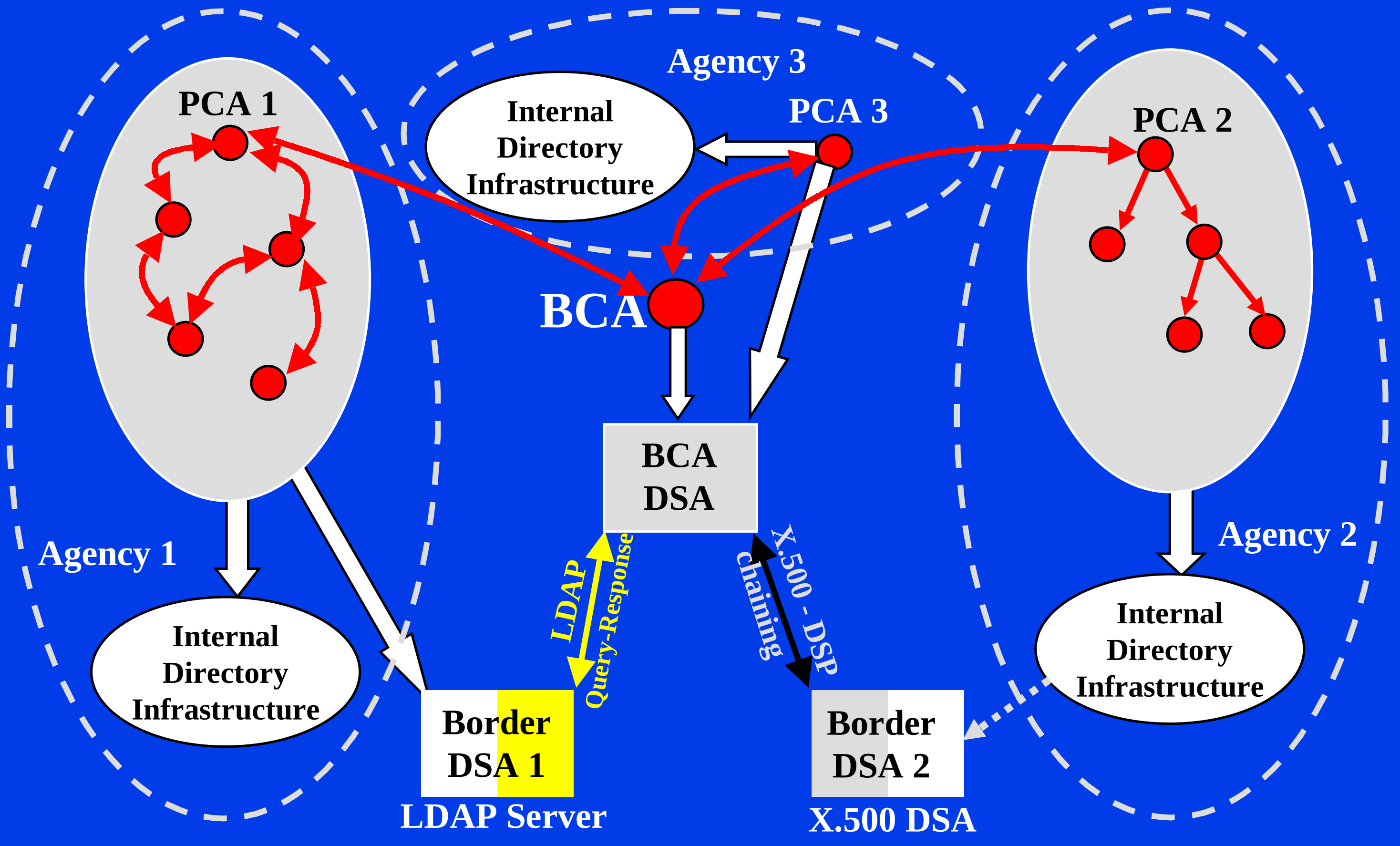
Bridge CA PKI Architecture



Directory

- Serves more than just PKI, but
  - Find certificates in a complex PKI
- The biggest single challenge in PKI
  - names, schema, chaining, protocols...
  - X.500 vs. LDAP server
    - right now only proven inter-vender server interoperability is via X.500 DSP
- Agencies often will not allow outside access to internal directories
  - Border directory concept

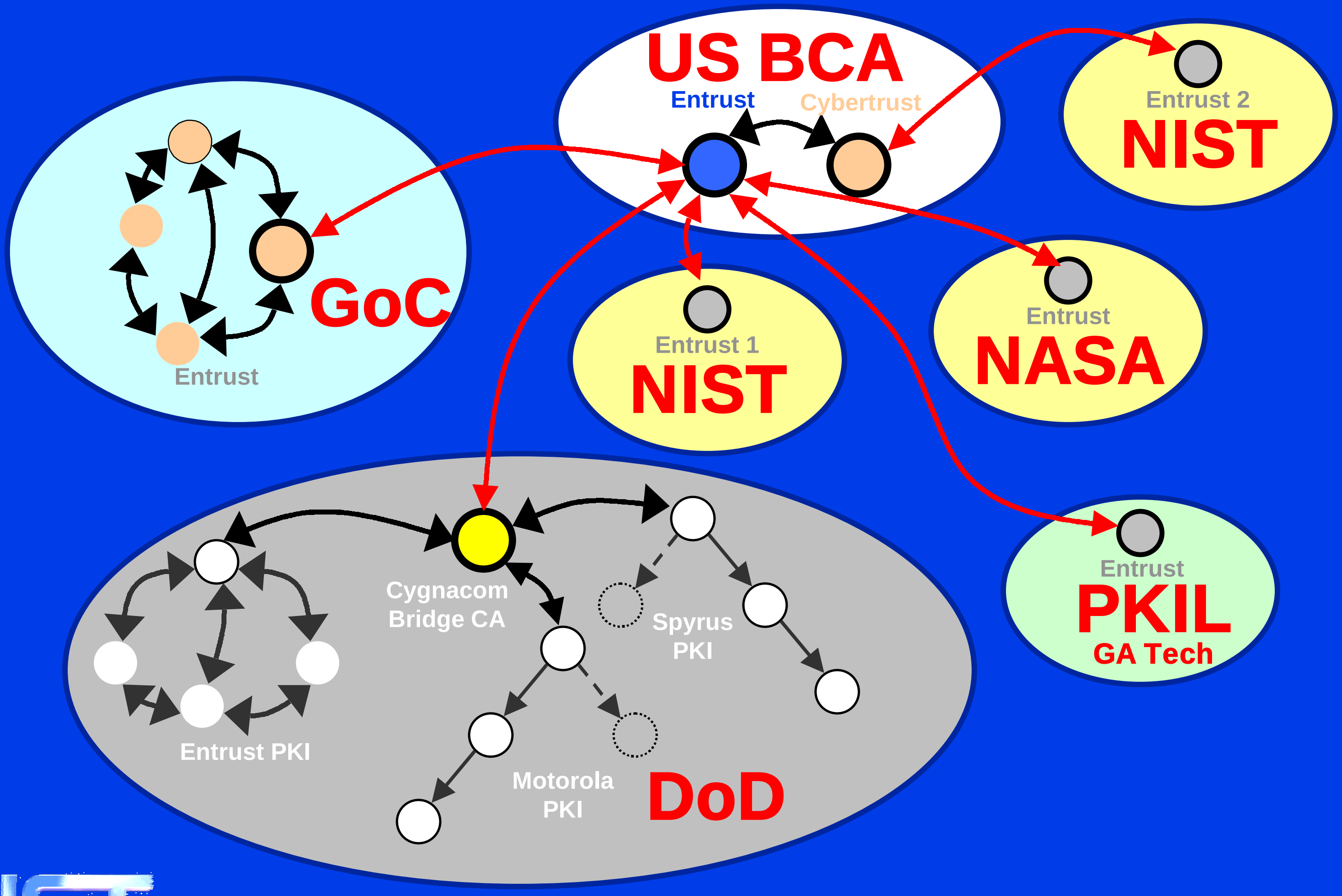
Expanded FPKI Directory



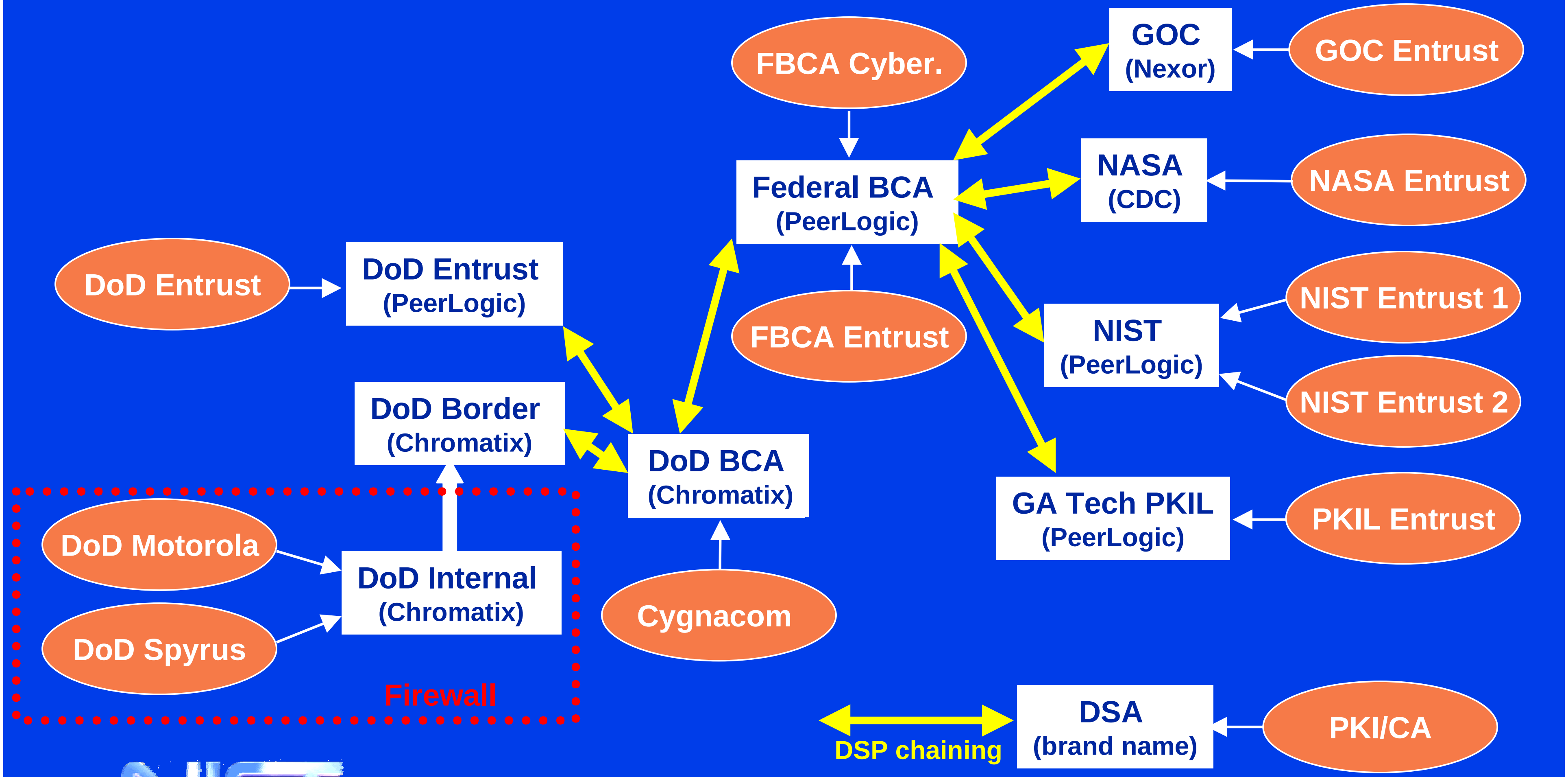
Federal Bridge CA (FBCA)

- FBCA Operational Authority
  - GSA
    - MITRETEK contractor
    - Entrust and Cybertrust CAs in prototype at the moment
- Challenge 2000 Demo
  - S/MIME application
    - freeware toolkits developed for path development and path processing
    - one policy level

FBCA Demo - Cert. Paths



FBCA Demo - Directory View



BCA Challenges

- Certificate chain building
- Cryptographic algorithms
  - RSA vs DSA & DH (or KEA in DoD)
- Certificate path processing
  - Particularly policies, including mapping
- Directories
  - Naming, schema, access control, protocol profiles, DSP vs. chaining and referral alternatives, LDAP

FBCA Futures

- Initial operational BCA
  - cross-cert. with operational agency CAs
- Possible incorporation of
  - Validation Authority
  - additional CA’s within the Bridge
- Consider more “LDAP oriented” directory chaining/referrals
  - domain component naming????
- Clients with cert. policy processing

Conclusion

- BCA approach offers prospect of large, diverse, scalable PKI
- Many challenges ahead
  - certificate path processing & policies
  - directories
- BCA demo is encouraging
  - biggest heterogeneous PKI yet demonstrated
  - useful freeware toolkits available

Questions????

Some URLS

- NIST PKI
  - » **http://csrc.nist.gov/pki/**
- FPKI Technical Working Group
  - » **http://csrc.nist.gov/pki/twg**
    - ◆ Bridge CA Demo Presentations
      - http://csrc.nist.gov/pki/twg/twg99_9.htm
    - ◆ FBCA Certificate Policy & FMPA Charter
      - http://csrc.nist.gov/pki/twg/Y2000/doc_reg_00.htm
- FPKI Steering Committee
  - » **http://gits-sec.treas.gov/oofpkisteer.htm**

Toolkits used in BCA Demo

- Freeware toolkits developed
  - Cygnacom
    - Certificate Path Development Library (CPL)
      - http://www.cygnacom.com/cpl/
  - J. G. Van Dyke
    - Certificate Management Library (CML)
      - **http://www.armadillo.huntsville.al.us/software**
    - S/MIME Freeware Library (SFL).
      - http://www.jgvandyke.com/services/infosec/sfl.htm

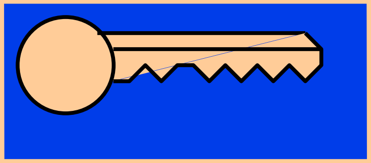
Federal PKI Committees

- Federal PKI Steering Committee
  - Rich Guida chair (Richard.Guida@cio.treas.gov)
- Fed. PKI Technical Working Group
  - Open meetings - industry welcome
  - Bill Burr chair (william.burr@nist.gov)
- Fed. PKI Legal & Policy WG
  - Michelle Borzillo co-chair (mborzillo@fdic.gov)
  - David Goldstone co-chair (david.goldstone@usdoj.gov)

Certificate Policies Extension

- Roughly speaking - a “certificate policy” may describe:
  - a “level of assurance” one can ascribe to a certificate, and/or
  - the community and applications the certificate is intended to be used for.
- Today, most clients ignore noncritical policies, & may not process policies at all.

Certificate Policies Extension

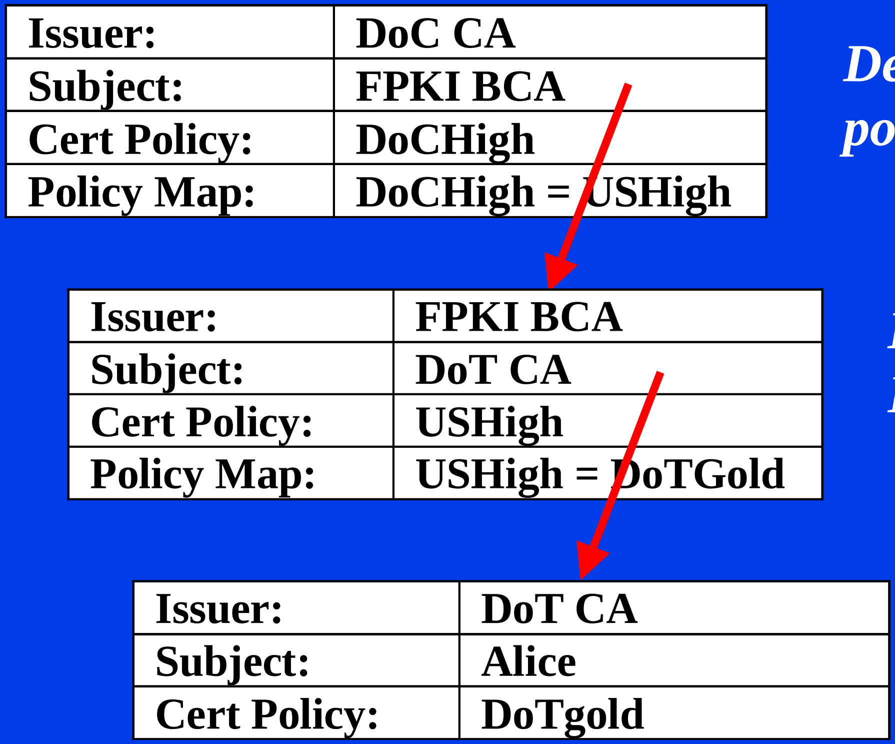
Name		Policy OID: (2)(16)(840)...	Signature

- Policy Object Identifiers (a series of integers) asserted in certificates by Certification Authority (CA)
- Related to Certificate Policy and Certification Practice Statement docs
- May be any number of policy OIDs in Certificate Policy field

Federal BCA Cert. Policy

- Four assurance levels planned
  - high, medium, basic, rudimentary
  - congruent with Canadian Gov. PKI
  - Draft: http://csrc.nist.gov/pki/twg/Y2000/doc_reg_00.htm
- FPMA will map from agency policy to BCA policies
- Client support for policy processing and mapping is major problem

Policy Mapping



Issuer:	DoC CA
Subject:	FPKI BCA
Cert Policy:	DoCHigh
Policy Map:	DoCHigh = USHigh

Dept. of Commerce maps its own policies to FPKI policies

Issuer:	FPKI BCA
Subject:	DoT CA
Cert Policy:	USHigh
Policy Map:	USHigh = DoTGold

BCA maps FPKI policies to Dept. of Transportation policies

Issuer:	DoT CA
Subject:	Alice
Cert Policy:	DoTgold

DoT asserts its own policies in Alice’s certificate